Ministry of Transport and
Communications

February 1998

DIGITAL SIGNATURES
– a technological and legal overview

Consultation paper by the Swedish interministerial working group on digital signatures

Ds 1998:14

Executive Summary

This consultation paper deals with problems and needs regarding digital signatures from a technological, administrative and legal perspective. The paper also includes some proposals for future action.

Digital signatures have already reached extensive use in Sweden. The paper describes among other things Swedish projects like *Allterminalen* (Total Terminal) and the work done within the SEIS association (Secure Electronic Information in Society).

In the paper's section dealing with legal aspects, the requirements of form according to Swedish law regarding written documents and signatures are described. Issues concerning evidence in IT environments are treated. The Commission on Computer Related Crime (*Datastraffrättsutredningen)* is touched upon regarding criminal and procedural law aspects, as well as legislation and proposals for legislation within administrative law.

The need for rules regarding content and effects of signature key certificates are analysed, as well as issues regarding certification and control of CAs. Questions regarding liability for the CA, the signing party, the trusting party and the State are discussed.

Finally some possible alternatives for action are outlined. So far, Sweden has restricted regulation of digital signatures to limited sectors. Existing proposals for general regulation of digital signatures have until now not led to legislation. If these proposals were complemented with a regulation of CA activity, a more extensive introduction of digital signatures would be facilitated. Society's need for effective law enforcement should be considered in this context, as well as Sweden's commitments regarding export of so-called strategic products.

Table of contents

1 Introduction to the English version

This consultation paper is a shortened version of the original Swedish version, *Ds 1998:14 Digitala signaturer – en teknisk och juridisk översikt*[1].

The paper has been put together by an interministerial working group of non-political representatives from the Ministries of Justice, Foreign Affairs, Defence, Transport and Communications, Trade and Industry, Finance and Interior Affairs. In working with the paper the group has been supported by representatives from the Swedish National Post and Telecom Agency, as well as a large group of external reference persons. Being drafted by non-political officials, the proposals of the paper do not represent formal Government policy.

The original report contains extensive discussions of most technical and legal aspects regarding digital signatures, including lengthy descriptions of international regulations. The parts chosen for translation here are those that deal with specifically Swedish aspects (corresponding sections of the original report put within parentheses): Use of digital signatures in Sweden (6.3), legal aspects (7.1, 7.3 and 7.4) and alternatives for action (10). With exceptions for footnotes and some other references to purely Swedish sources, these sections have been translated in full.

Observers wishing to submit opinions on the text are welcome to so no later than April 20th 1998 to the following addresses:

Ministry of Transport and Communications
S-103 33 Stockholm

Telefax: (46)-8-411 89 43

E-mail: registrator@communications.ministry.se

[1] Both the Swedish and the English versions of the paper can be found on the following Internet address:
http://www.regeringen.se/info_rosenbad/departement/kommunikation/ds98_14/

2 Market developments in Sweden

During 1995, the project 'Strategic co-operation relating to electronic ID within the bank and finance sector' was completed. The objective of this project was to develop a shared technical solution for an electronic ID card to increase security levels within a number of electronic services. The specifications for the solution were made generally available.

The co-operation between the Swedish National Police Board, the Swedish Defence Authority, the Swedish State Office, the Swedish Insurance Office, the Swedish National Tax Office and the Data Inspectorate relating to the so-called *Allterminalen* (Total Terminal) is the next step in the development process. In this work, the specifications are applied to a modular security environment for personal data protection. Special security cards (so-called AT cards) form part of the solution. The cards are smart cards ("active cards") configured using codes for a unique electronic identity, digital signing and support for encryption.

In the spring of 1995, the Secure Electronic Information in Society (SEIS)[2] association was formed. Through the formation of the SEIS, work was continued with the objective of developing a framework for widely accepted, simple, practical and economic security solutions. All sections of society are represented in the association.

The work by the SEIS involved the refining and augmentation of the technical specifications for the basic security functions of electronic identification, digital signatures and support for encryption on active cards. SEIS is considering the conversion of relevant sections of the specifications to the Swedish standard during the spring of 1998, when these standards are due to be revised and harmonised with regard to international use on the Internet, etc. SEIS has also developed regulations ("policies") for the issue and certification of electronic ID cards (with chips) which will also be compatible with the relatively newly established SIS[3] standard for ordinary visual ID cards. Work is also under way within SEIS to establish a policy for the presentation of "SEIS cards" in order to be able to guarantee that a card holder does not receive the same identity or details as another card holder. Consideration is also being given to the requirements to be placed on certificate catalogues, etc in addition to other issues relating to security in a public key infrastructure.

In June 1997, the so-called Top Management Forum *(Toppledarforum)*[4] accepted a proposal for a common IT security solution in State, municipal and regional governments. The solution is based on the official use of

[2] See http://www.seis.se
[3] SIS: The Swedish Standardisation Institute
[4] See http://saturn.nutek.se/ (Swedish language only)

active cards with the three basic security functions in accordance with SEIS specifications. The work involving the establishment of routines etc., for the issuing of these cards was begun by the State Office in the autumn of 1997.

The Defence Authority has a security system which involves the use of active cards for identification, digital signatures and encryption during the transmission of messages. The system was developed during the period 1994–1995 in accordance with the relevant standards and specifications. Other aspects relating to the actual use of AT and SEIS cards are presented below.

2.1 The use of AT cards for digital signatures

The Customs Authority probably has the greatest experience of digital signatures in the form of seals based on symmetric encryption. As early as 1991, the Customs Authority began to offer companies the opportunity of digitally signing transactions for import and export declaration. A gradual transition to Total Terminal solutions and the associated AT cards has taken place since 1997. The Customs Authority issues the relevant cards to each company. Approximately 700 cards are currently in daily use by 500 companies with the Customs Authority's permission. Three quarters of the total number of declarations are handled entirely by electronic means. The Customs Authority has chosen to work without CA.

The Swedish National Tax Office has also chosen the *Allterminalen* solution. The number of AT card users is today approximately 13 000, of which approximately 3 000 are within the enforcement service. When the solution has been fully implemented in 1999, it is estimated that the total number of users will be approximately 15 000. About 250 local employees are connected to a central database (common to all tax authorities) for the issuing and certification of AT cards. The card's functions are currently used for local PC protection – the so-called strong authentication (authenticity verification) and line encryption. Functions for the digital authorisation of decisions in Magi, the tax authority's new tax and toll system, will be introduced in February 1998.

The Swedish National Police Board has also chosen the *Allterminalen* solution. It has introduced approximately 15 000 stationary and 2 000 mobile workstations with a total of about 25 000 card users. During late 1996 and early 1997, a successful trial was carried out using digital authorisation (using AT cards) and the transmission of encrypted analysis results from the State Criminal Technical Laboratory to the Police Authority in the county of Stockholm. However, the processing of the prosecution authority documents required that electronically signed documents be printed out on paper. Depending on the prosecution authority's requirements for the printing of electronically transferred information, the Police Board will therefore not be using the AT card's functions for digital signatures in its work for the time being.

Within the area of national insurance, the Swedish National Social Insurance Board was responsible for the introduction of a total terminal solution during 1997. This work involved a total of approximately 15 000 workstations. The need for digital authorisation is expected to increase in order to simplify and optimise activity in the future. AT cards have so far however only been used for identification purposes for computer systems. Administration of the insurance funds and the certification of AT cards are managed by the Insurance Office's central computer department. No date has yet been set for the introduction of digital signatures within the organisation.

Danderyds hospital in the county of Stockholm has recently introduced a security solution equivalent to the *Allterminalen* solution to control and administer case records and other information. As with the authorities described above, the relevant active cards are issued under the hospital's own jurisdiction by the security department. The scheme has worked well. In the long term, digital signatures can be integrated with the case record system for the legal signing of case records by doctors. This however requires further development of the applications.

2.2 Use of SEIS cards for digital signatures

Within the healthcare sector, co-operation is currently taking place between the county councils in the Skåne, Väst-Sverige, Östergötland regions as well as in Huddinge hospital in Stockholm county council for the development of a text model for digital signatures using active cards configured to SEIS specifications and supplied by the Swedish Post Office. The healthcare development institute Spri is involved in the work and it is intended that testing of the model for the signing of travel expenses for fifty users will begin during the latter part of 1998. Discussions are also under way relating to the digital signing of case records using active cards for official use. Skåne county council seems to be most advanced in this regard with plans for implementation in early 1999. With regard to this, it should be noted that an algorithm standard for digital signatures within the health and healthcare sector was established by the European standardisation organisation CEN (ENV 12388).

In March 1997, the Central Study Support Committee (CSN) gave students at the Royal Institute of Technology in Stockholm (KTH) the opportunity of digitally signing the spring term's obligatory mid-term inquiry or declaration using the signature function on the students' IDOL cards (ID orientated solutions) [5]. During the autumn of 1996, students at KTH were issued with active cards containing the three basic security functions in accordance with SEIS specifications as part of a wide-ranging trial by KTH, the Swedish Post Office, Telia, Tryggbanken and

[5] See http://idol.promotor.telia.se/

others. The use of digital signatures for confirmation to the CSN regarding current studies was very successful both technically and practically. Encouraged by this experience, the CSN wants to develop the solution's potential to include applications, the completion of applications and the handling of other procedures relating to studies. Any large-scale developments must however wait until the legal aspects of digital signatures and related issues have been clarified. The CSN also sees advantages in the use of digital signatures both within committees and in co-operation between committees and other authorities.

Many county councils and municipal authorities have comprehensive plans for electronic commerce. Dalarna county council are, for example, very advanced as more than ten years ago the council began to develop plans for radically changing procurement procedures for consumables in the hospital sector using digital techniques. Today all orders for the supply of materials are collected in the county council's system and then forwarded to the council's own warehouses or the relevant supplier. The work on developing electronic trading is the Top Management Forum's most comprehensive project and intensive work is currently underway to further this development in many areas. The State sector has also begun work. The open and general interfaces for security solutions which the project's security group has developed are based on the use of active cards with the three fundamental security functions – electronic identification, digital signatures and support for encryption in accordance with SEIS specifications. The potential for legally acceptable digital signing is believed to be an important factor in the future of electronic trading.

The Swedish Financial Supervisory Authority regularly tests the electronic transfer of information from approximately ten banks and insurance companies. Personnel at the banks and insurance companies have been issued with active cards supplied by the Swedish Post Office. Two of the cards' functions are used in the trial – electronic identification and support for encryption. The use of digital signatures has not been considered necessary for the secure identification and transmission of information from banks and companies to the Finance Inspectorate. The trial is to be extended. It is anticipated that there will also be an internal requirement within the Finance Inspectorate for digital signatures.

Since 1997, the Nordbank has issued personal active cards conforming to SEIS specifications to about 10 000 customers, either with or without photographs depending on the customer's wishes. All three basic functions (identification, authentication and encryption) in the card are used for the bank's Internet services for applications for loans, new accounts and access to capital savings. The solution is in full operation. Loans have for example already been issued – entirely without "paper".

In co-operation with several banks, the Bank giro centre is developing a solution for secure electronic payments to be used between company

financial systems and the bank giro system. The security functions consist of secure electronic identification, digital signatures and support for encryption using active cards in accordance with SEIS specifications. The pilot scheme is due to be introduced during the first quarter of 1998.

In co-operation with the Stockholm City Planning Committee, Stockholmshem and the Post Office, the company SignOn is developing an Internet application which enables the regulatory and obligatory minutes of discussions to be sent electronically from Stockholmshem to the Stockholm City Planning Committee. The trial is due to begin in March 1998. The trial will involve the use of active cards in accordance with SEIS specifications. The cards will be supplied by the Post Office which will also be responsible for the security platform (the so-called CA functions, etc). In practice, SignOn is converting the standard forms to electronic documents, which are then made available on the Internet.

The electronic forms are completed by personnel of the relevant department at Stockholmshem and then signed digitally by an authorised person using the personal card's signing function. The electronically signed form is then returned and made available to the Stockholm City Planning Committee via the Internet. The system is believed to be the first of its type in the world.

2.3 Use of digital signing and verification at the Handelsbank

The Handelsbank also has a solution for the digital signing of private bank transactions via the Internet. The Handelsbank has however chosen a different solution to the use of physical actual active cards. Through a connection via the Internet to the Handelsbank's system, the bank's customers can download special software which enables them to create their own certificate containing a secret code and at the same time generate equivalent open codes. When this has been done, they are sent electronically (via the Internet) to the bank's security system so that the certificate can be authorised by digital signature in the bank. When the customer's certificate has been signed by the appropriate authority in the bank, it is returned to the customer's system (PC) where the certificate will be kept. As the bank has access to the customer's open code, the customer can at a later stage, if desired, use the digital signature in future communications with the bank.

2.4 Secure electronic transactions – SET

SET (Secure Electronic Transaction) is a technical specification which has been developed to facilitate payment by credit card via the Internet and at the same time use existing account structures. The work, which began in 1995, is being carried out by VISA and MasterCard in co-

operation with leading software suppliers. The specification regulates on transactions, transaction formats, certification of all parties involved and rules on how information is protected in terms of secrecy, integrity and source control. Transactions are signed digitally by special software by the account-payment card owner and the shop owner. The signature is verified when the transaction reaches the bank.

Within SET, agreements are drawn up between the card-issuing bank and the account cardholder and between the bank and the point of sale. The system is therefore complete in that it builds on agreements between all partners involved.

The trial has been initiated and operated jointly in several European countries. A Swedish trial is to be introduced in co-operation with VISA, FöreningsSparbanken, Handelsbanken, Postgiro Bank and the SE Bank. The trial is estimated to involve 8 000 private customers and forty sales points. The trial in Sweden has been delayed several times.

3 Legal aspects

3.1 Areas of legal interest – overview

3.1.1 Regulations concerning requirements of form

In some legal rules, requirements are laid down on legal documents being produced in a certain form in order to be legally effective. Some of the most common requirements of form are, *written format, personal signature* and existence of a document in the form of a physical *original*. In the requirement for personal signature, it may also be implicit that there should be a personal signature and a physical original of the document in question.

The effects of non-fulfilment of form requirements can vary. In some cases the requirement is absolute for the validity of the document. In other cases, deviations from the requirement that a document be in written form can involve commercial/legal sanctions. Sometimes the legal effects are intrinsic to the document as such; the person who possesses the document also possesses the rights which the document contains. This applies chiefly to so-called negotiable instruments, e.g. promissory notes, bills of exchange and cheques.

The main reason for the form requirements are legal safety and effectiveness in significant economic – or other – activities. This includes amongst other things, providing evidence that an action has actually taken place, by whom it was carried out, and of what it consisted. Another reason is that the state, by setting form requirements, can facilitate procedures in certain activities, e.g. taxation. The form requirement can also serve as a warning, thereby insuring that a party is aware of the consequences of a particular legal action.

Form requirements vary from country to country. In international transactions, the question therefore arises as to which country's form requirements apply. The question of the form of contracts has a special position in international civil law. A legal document's form is considered valid either if it fulfils the form requirements of the country whose law applies to the contract, or if it fulfils the form requirements of the law in the country where the legal action was carried out (some exceptions exist though, in accordance with article 9 of the Rome Convention) In electronic communication, problems can arise in determining where a legal action took place.

Electronically transferred information (electronic documents) differ from traditional paper documents in several respects which have a direct bearing on their legal status. In cases where a statute stipulates a signature, an electronic document will probably not suffice.

In order to ensure that digital signatures are accorded the same legal significance as traditional signatures, it is likely that the rules which stipulate form need to be changed so that digital signatures – which are created with a required degree of security – are accorded the same status as personal hand-written signatures. Since the motives behind form requirements may differ between laws, a general rule equating digital signatures with hand-written signatures is not possible. Acceptance of digital signatures would have to be tested statute by statute. In order to obtain an overview of the regulations which contain the requirements of written form and signature, an inventory of all Swedish legislation, agreements with foreign countries and EU regulations is necessary. This however would lead to quantities of information too large – at least in the context of this consultation paper – to permit detailed analysis of which rules can be applied in connection with digital signatures. In a database-search, the so-called IT-investigation[6] found that the words "sign" occurred in 562 statutes whilst "in writing" occurred in 1095 statutes.

Swedish legislation contains a number of statutes requiring that actions be recorded in writing or signed. Below are just a few laws which require the presence of signatures.

- Documents legitimising the transaction shall be signed by the vendor and the purchaser when transferring real estate (chapter 4, paragraph 1 Land Code).
- Powers of attorney to represent a person in court shall be signed by that person (Chapter 12, paragraph 8 of the Code of Judicial Procedure).
- Annual accounts shall be signed and dated by the person responsible for their compilation (paragraph 11 of the Accounting Act).
- Signatures on behalf of companies shall be accompanied by the full business name of the company and the name of the company signatory (paragraph 26 of the Trade Names Act).
- Wills shall be signed by the testator in the presence of two witnesses (Chapter 10, paragraph 1 of the Inheritance Act).

The IT-investigation was initiated in May 1994 with the objective of scrutinising the use electronic documents in business and public administration. In March 1996 it presented proposals for changes in legislation, changes that include the use of digital signatures. These are currently under consideration by the Ministry of Justice.

[6] "IT-utredningen", SOU 1996:40 Elektronisk dokumenthantering (Electronic Document Processing)

3.1.2 Questions of evidence

3.1.2.1 General

Even in cases where written format or personal signatures are not a formal requirement, both are very important in relation to evidence. The difference between a signature on paper and a digital signature however should have less significance in this context than the form requirement.

The administration of justice in Sweden is based on the principle of the *free assessment of evidence*. No limits are placed on sources of knowledge which may be used – the presentation of evidence is free. When evaluating evidence, a judge is not bound by any law – the evaluation of evidence is free. There is therefore, in Swedish law, no bar to the presentation or consideration of IT-material as evidence.

Under normal circumstances it is unimportant whether a document used in evidence is presented in its original, as a copy or as an excerpt of a record in a case. The problems are more of a practical nature.

- How are facts ascertained in the IT-environment? There may be uncertainty as to the origin or reliability of information.

- The evaluation of IT-material in a case can be technically complicated. How should a person trading on the Internet, for example, go about facilitating the proper evaluation of evidence? Who should be regarded as the issuer of a potential document? Who is considered to have "supplied" the relevant information when new compilations of information are generated using other search-criteria than those intended?

- How can the need for experts on relevant information systems be ensured?

These questions are dealt with in more detail in the Commission on Computer Related Crime[7] and in the Council of Europe's recommendation No. R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology.

3.1.2.2 Burden of proof where questions of forgery arise

In case law has been ruled that if a debtor contests the authenticity of a document, it is for the creditor to show that that document is genuine. If, on the other hand, a debtor maintains that a document is indeed genuine but that its text has been altered, (so-called content-forgery), the debtor retains the burden of proof in substantiating this.

[7] Datastraffrättsutredningen, SOU 1992:110

The question of whether this application of the burden of proof should also be used in cases involving the forgery of purchase notes used with credit cards – which are neither valuable documents nor ID-papers – has been tested in a 1992 court case[8]. The Swedish Supreme Court ruled that it was the responsibility of the credit card holder to demonstrate that forgery was at least probable. If this requirement is fulfilled, according to the Supreme Court, the credit card company must demonstrate that the purchase note is genuine in order for its case to be upheld. This rule, according to this case, applies both to content forgery and the forgery of signatures.

3.1.3 Questions of civil law

This section deals briefly with issues relating to standard contracts and patents. Questions of liability in different party relations are discussed in section 3.3.6.

3.1.3.1 Standard contracts

The type of standard contract which occurs today in the IT-environment (so-called EDI standard contracts) normally does not include any regulation of digital signatures. One can assume however that the traditional EDI communication, which today occurs in closed systems, will be replaced to a certain extent by communication via open networks. Digital signature technology makes it possible to avoid many of the disadvantages of communication via open networks. If development moves in this direction, parties who have continuous contractual relations will be able to regulate dealings with digital signatures through contracts. For others this would appear more doubtful. It is possible that other groups too will be included in standard contracts which regulate digital signatures, for example, in an electronic marketplace where all participants have bound themselves to the marketplace's contractual conditions.

There are standard regulations for CA activity, the so-called Certification Practice Statement, CPS – in which the technology used by CA's, processing routines and the scope of CA's responsibility is usually made clear.

3.1.3.2 Patents

Signature and hash algorithms are used for signing with digital signatures. These algorithms can be protected by patents. Certain functions and components which are important for the technical implementation can also be patented, e.g. in the area of smart cards. If legislation concerning the technology used for the production of digital signatures is deemed

[8] NJA (*Nytt juridiskt arkiv*) 1992 p. 263

necessary, the use of patent protection will have to be taken into consideration in connection with this.

Implementation patent for IC-cards

There is a patent on the technology which makes it possible to use only one digital signature per activation. In order to sign again, the card has to be activated again by the its owner. The most relevant algorithms are the following:

Signature algorithms. These exist in two forms.

- RSA, which is also used for so-called public key-encryption, is the best known and most used algorithm for digital signatures. It is internationally standardised (ISO, ISO/IEC). It is patented in the USA but can be used freely in Europe.

- DSA, which is included in the American signature standard DSS. It is also patented. NIST, which was behind the launch of DSA, has however stated that it will be offered free of charge on the world market. DSA is however the subject of a patenting dispute and, at the time of writing, it is unclear whether the dispute has been resolved.

Elliptical curves: This mathematical basis for creating new and more effective signature algorithms has not been patented for signature use. Many effective uses for elliptical curves have however been patented.

Hash algorithms: The most common hash-algorithms, which occur in connection with digital signatures, are not patented.

3.1.4 Questions of criminal liability and litigation

The adaptation of criminal liability to the IT-environment

The question of legal protection in the IT-environment has already been dealt with by OECD[9] and the Council of Europe. The Council of Europe has produced a recommendation[10] concerning activities which should be criminalised.

Certain changes in law have been passed in Sweden in order to provide legal protection in the area of IT; partly in connection with the introduction of the Data Act, partly in connection with a recommendation

[9] OECD Report No. 10, Computer-related Crime: Analysis of Legal Policy, 1986
[10] Recommendation No. R(89)9 on Computer-related Crime and final report of the European Committee on Crime Problems, 1990.

in the Crime against Property Report[11]. Sweden has thus obtained legal protection against criminal behaviour in the IT-environment specifically.

In one area however, which is of particular interest in relation to digital signatures, no changes in the law have been made. This is the question of crimes involving documents.

Swedish law on crimes involving documents is mainly designed to protect the reliability of evidence. In principle, it is obvious that digital documents which are intended as evidence are just as worthy of protection as paper documents. This point of view was expressed in the Council of Europe report mentioned earlier. The report recommends the criminalisation of forgery in the IT-environment, equating such forgery with forgery involving traditional paper documents.

The Commission on Computer Related Crime

In order to illuminate the discussion about the criminal law aspects of digital signatures the Commission on Computer Related Crime's points of view are related briefly below. The Commission's work is currently under consideration within the Swedish Government Offices.

Legal sanctions against forgery under current law relates chiefly to paper documents and the information these contain. In case law however, under the pressure of technological development, certain electronic documents have been accepted as documents in the normal sense of the word. This has happened in spite of the fact that the unavoidable authenticity testing of the objects in question has only been possible through procedures which are not normally acceptable under the Criminal Code. Sometimes therefore, cases have reached the limits of what can be considered legally acceptable analogy. It is therefore unclear at the moment how much legal protection digital documents actually have. If there is a need for legislation in this area, consideration should be given to how far this can be provided through the adaptation of current rules in the Criminal Code and/or to what extent special legislation is required. In relation to the freedom from national borders enjoyed by digital documents, it would be reasonable to consider the harmonisation of legislation internationally.

In order to provide legal protection for a document – irrespective of whether it is of the digital or traditional type – it is necessary for the document to contain some form of evidence of its originator which it is possible to legally link with anyone alleging that he/she produced it or with anyone falsely alleging that someone else produced it. It must also be possible to test the authenticity of the document. The difference between digital documents and traditional paper documents in this respect is the difficulty in establishing whether, and to what extent, the former have been corrupted. In contrast with paper documents, the content of a digital

[11] Förmögenhetsbrottsutredningen, SOU 1983:50

document is not bound to any physical medium and can normally be stored, reproduced and changed without this being detectable. Creating the possibility of such detection is one of the main objectives of a digital signature.

In order to be able to provide a digital document with legal protection against, for example, forgery, there has to be a procedure in order to "lock" or fixate the content of the document so that changes in the document cannot be made without being detected. As in the case of ordinary locks, it is doubtful whether any digital lock will ever be produced which offers absolute protection against intrusion. This in itself should not be a barrier to providing legal protection for digital documents. The question is rather which requirements should be placed on a digital lock in order for digital documents to be given legal protection. Another important question is the extent to which manipulation of a document must be proven in order to attain legal protection. Another question which requires clarification is whether there is reason to differentiate between degrees of legal protection so that digital documents which do not fulfil the requirements for acceptable digital locks are not left completely without legal protection.[12]

Any legislative solution to these problems should be framed in such a way that those checks which are currently possible in the IT-environment can be used and that their future development is not hindered.

Digital signatures

The purpose of digital signatures is to establish *who* produced the digital document and that the *content* of the document has not been manipulated.

In order to successfully create a system of digital signatures, the concept must already have the trust of the public. This means not only a choice of technology which offers high security, but also adequate criminal sanctions against abuse of that technology.

The work currently in progress in SEIS aims at creating digital signatures with so-called smart cards, whose functions are "opened" with the help of PIN-codes. The smart cards will have the same exterior format as normal ID-cards. The holder is expected to memorise the PIN-code and keep it secret.

As long as the card is only used in the traditional manner (i.e. manual control of the card-holder's identity) the current procedures for issuing

[12] The Commission on Computer Related Crime has proposed that digital messages which do not fulfil the checking criteria should be given only limited legal protection. This, according to the Commission, can be provided through the introduction of a new law on liability for *misuse of a document*. The inquiry proposes that liability be incurred first when the object is used.

and using ID-cards should be applied. For these objects there is both legal protection and functioning agreements between the parties.

The question is however how protection for the PIN-code and the digital data stored in e.g. a chip with which a smart card is equipped should be viewed. Under current Swedish law, it is not a crime to covertly discover and utilize someone else's password. The Commission on Computer Related Crime has therefore proposed a new rule on the misuse of passwords[13]. A question that arises is in which cases a chip with stored data will be covered by the definition of document.

How, moreover, should one regard an action where someone other than the person to whom a digital signature is issued makes use of the smart card and the PIN-code? It is just as difficult to check who has made a withdrawal from a cash-point as it is to check who used a certain digital signature. It is of course possible to establish to whom the signature was issued, but not who used it, and even less whether this was done with the owner's consent. This limitation in combination with the potential of areas in which the signature can be used, gives rise to the question of whether all use of digital signatures by persons other than those to whom they have been issued should be criminalised.

Another type of misuse against which criminal sanctions could be considered is where someone who has set his/her signature on a digital document later denies this. However secure the relevant procedures may be, a denial of such signatures always gives rise to uncertainty and extra work. Such behaviour should perhaps therefore be criminalised in the same way as in the traditional environment.

Sanctions in criminal proceedings

The question of criminal proceedings is closely connected with criminal law. This is because the authorities dealing with crime can, in certain instances – through decisions taken by a court, a public prosecutor or the police – be given powers to take steps which are not normally permissible by authorities. In this respect, criminal law and criminal procedural regulations are characterised by a delicate balance between protection of the rights and freedoms of the individual on the one hand and, on the other, a public interest in providing protection against certain types of crime. This touches upon Sweden's international obligations, the Swedish constitution and ordinary law. Corresponding questions relating to digitally stored documents also need to be answered.

[13] "Any person unlawfully using a password or other secret identification information, which can give access to data for automatic information-processing, with the intention of passing him/herself of as being a certain person or passing on such identification information for misuse in the aforementioned manner, will be convicted, if this leads to danger in relation to evidence..."

The question of adapting the rules of criminal proceedings to the IT-environment has been dealt with by the Commission on Computer Related Crime. The Police Law Commission also touched on these questions in its final recommendation (SOU 1995:47 Sanctions according to chapters 27 and 28 of the Code of Judicial Procedure and to the Police Act). Proposals based on these inquiries are currently being prepared by the Ministry of Justice. Other matters relating to sanctions in criminal proceedings which could affect the IT-environment are dealt with in the Bugging Report (JU 1996:07, dir. 1996:64).

Questions concerning criminal proceedings related to information technology have also been dealt with internationally. The Council of Europe has adopted a recommendation on the subject and work is currently going on with the objective of creating a convention for international co-operation in this area.

3.1.5 Legal questions concerning administration

The Administrative Procedure Act does not require a message submitted to an authority to be signed by the sender. According to section 10, paragraph 3 of the Act, the authority may, however, require that the message that has not been signed be confirmed by the sender through a personally signed document. Requirements of documents being signed exist in special statutes (*lex specialii*), which take precedence over the Administrative Procedure Act (section 3 of the Act).

3.1.5.1 Electronic documents in Swedish legislation

At present, electronic documents are included in just under thirty Swedish laws. In these, an electronic document is defined as a document whose content and originator can be defined by a certain technical procedure. The use of electronic documents is chiefly regulated within the areas of customs and tax, by the enforcement authorities and in the registration of mortgages. Parliament has directed on three occasions that there must be a general solution to the question of electronic documents used in administrative procedures.

In both the customs and tax areas, special permission from the recipient authority is needed for information required by law to be submitted in electronic format. The Swedish Board of Customs has laid down detailed instructions on the submission of electronic information in the regulations (TFS 1994:45) on the application of customs laws and regulations.

The background to changes in legislation on electronic documents concerning taxation can be found in a 1994 Finance Ministry report[14] and in a 1994 Government Bill (prop. 1994/95:93). It was proposed that an

[14] Ds 1994:80 Elekronisk dokumenthantering i skatteförvaltningen (Electronic document management in tax administration)

electronic file may contain all documents on a matter, both electronic documents and electronic reproductions of paper documents. It was proposed that electronic documents produced in the Tax Authority be legally equivalent to paper documents in law. From 1998 onward the National Tax Office or local tax authority can permit tax declarations to be submitted in electronic form. Hitherto, only appendices to declarations, which do not require signature, have been allowed in an electronic format specified by the National Tax Board. This format consisted of a smart diskette called ELDA. In the ELDA system, the sender keeps a diskette with a certificate and private and public keys. The diskette also contains the software which the user needs to communicate with the tax authority. The National Tax Board is working on the development of web-based technology for collecting information. This is included in the so-called IN/OUT computer platform. The National Tax Board intends to create a secure method of communication using standard software for the Internet with the SSL-protocol or stronger encryption.

3.1.5.2 Archives

Archives, used here as the name for a function rather than for premises or stores of documents, have for centuries been a guarantee that papers documenting rights and obligations can be preserved. Over this period this function has also undergone changes, from being connected with legal questions to being linked mainly with the scientific or cultural aspects of the papers preserved. This has lead to the meaning of archives and the rules governing them being underestimated as part of the preservation of legal security. In recent years however the legal significance of archives has been recognised in legislation.

The current law governing archives (1990:782) came into force on 1 July 1991. In connection with this, the National Archive issued a new set of rules (RA-FS 1991:1 etc.) which contained partly revised rules and partly a codification of practice for archives. The rules deal with all aspects of the formation of an archive, from the production of documents to rules for the design of archive premises. The basic requirement of the rules is media-independence and applies to all types of documents; paper, computer-generated records, microfilm etc. The rules are also designed in such a way as to avoid unnecessary control of detail, instead allowing the archiving authority to use production methods which suit their purposes. The only limitations are that documents produced should be legible and transferable to new modes of storage over time without certain important qualities being lost.

On the production of computer-generated records

The following purposes for archives are laid down in the Archive Act.

– Authorities' archives are part of the national cultural heritage.

– Authorities' archives shall be preserved, kept in order and cared for so that they maintain the right to examine public documents, the requirement of information for the administration of justice and the needs of research.

In order for these objectives to be fulfilled, and it should be noted that there is no time limitation in the above, it is necessary that authorities use suitable methods and materials for the preservation of archives. (paragraph 5).

The use of computer-generated records for archives and the production of documents can involve numerous problems. In order to counteract manipulation, unintentional changes etc., systems are required for authorisation, safety copying and the preservation of copies in different places. The lack of permanence in data-bearing material has been dealt with by regular transference to new data-bearing material. Using this strategy it has also been possible to deal with the fact that technical equipment quickly becomes obsolete because of the speed of development.

The speed of technological development also creates another problem, namely the large number of formats for data in the form of font-ranges, file formats, compression methods etc. The steps taken to ensure preservation in this respect are based on a different strategy from the one used for physical data-bearers such as parchment and paper. Securing the logical permanence, i.e. preserving the content of computer-generated records has been achieved through the National Archive stipulating that computer-generated records which are to be preserved must be produced in accordance with international, European, or national standards, or be convertible to such standards in order to guarantee long-term preservation. These stipulations are only binding when computer-generated records are transferred to the archiving authority. In other cases these should be seen as a (strong) recommendation when submitting computer-generated records for long-term preservation by an authority (i.e. when the information is no longer required for the activities of the authority). Since most types of computer-generated records (e.g. registers, word-processor documents, e-mail messages etc.) do not normally have properties which can be lost during conversion, most preservation problems have hitherto resolved.

On the properties and thinning of documents

Those qualities which are decisive in establishing whether a document is considered authentic and reliable are dealt with in the archive/scientific discipline of diplomatics, which has its origins in medieval Europe. Today it is more common for these questions to be dealt with in crime laboratories and courts than in archives. But traces of diplomatics can be

found both in the rules which were summarily dealt with in the preceding section and in the definition of thinning which is used in the rules of the National Archive.

Thinning – destroying public documents or information in public documents; destroying such documents/information in connection with transfer to another data-bearer is considered to be thinning if the transfer involves the loss of data, the loss of data-collation possibilities, the loss of possible search opportunities or the loss of the ability to establish the authenticity of the information.

In this instance it is the loss of the ability to establish the authenticity of the information (i.e. document) which is of interest. This should be balanced against the objectives of the Archive Act listed above. In relation to transfers between authorities, it should be possible in theory to guarantee that digitally signed computer generated records can be preserved in their original formats. Authorities should be able to come to agreements on long-term legible formats. Alternatively, the National Archive could lay down regulations on such formats. It would be difficult, if not impossible, to introduce binding rules on the technical formats allowed – when the public submits information or documents to authorities in the form of computer-generated records – to the Administrative Procedure Act (1986:223) as a supplement to the rule (section 10, paragraph 3) on the right of authorities to demand personally signed documents. Regarding digital documents created by individuals, the main rule will be ”thinning to preserve” in those cases where no particular requirements of form is put by the authority. Increased costs for preservation (due to increased need for conversion and less possibilities to establish who the originator of a digital document is) can arise as a result of this.

Different roles in the production of conventional documents

In dealing with the relationship between authorities, the National Archive and Certification Authorities, it might be of interest to know something about relationships in the more conventional environment. Here the National Archive lays down requirements to authorities. The authorities must then conform to the technical requirements on paper-qualities, the production of reprographic copies etc. Requirements are thereby placed indirectly on suppliers. The National Testing and Research Institute or other accredited certification body checks whether products and services used fulfil the National Archive’s requirements. The accreditation body SWEDAC checks in turn that the National testing and Research Institute fulfils the requirements which placed on a certification body (e.g. premises, documentation, training of personnel etc.). The National Archive and regional archives check finally that the authorities use products which fulfil the National Archive’s production requirements. As an alternative to certification, a so-called suppliers assurance can be used.

This procedure is however conditional upon requirements being placed on supplier's internal quality-control systems.

3.1.6 International civil and procedural law

Digital signatures will to a large extent be used for electronic communication across national boundaries. Irrespective of the purpose of the communication (electronic commerce, transmission of information, transmission of money etc.), problems of a legal nature will arise. When such problems arise in connection with trans-border communication, questions will also arise regarding which country's laws will apply and which country's courts will be authorised to resolve disputes.

Rules based on international civil and procedural law provide solutions for such problems. A survey of legal rules of importance for the use of digital signatures would be incomplete unless these rules are mentioned.

The problems of an international civil law character that are of greatest interest deal with the issue of which country's law that should decide if a contract with international implications has been drawn up according to the correct form.

Along with the increased internationalisation of trade, international civil law problems are ever more often brought to the fore. This is probably the reason why international organisations such as UNCITRAL and EU not only se it as an important task to co-ordinate regulations of infrastructure for digital signatures, but also find it important to explore the extent to which countries' national legislations on digital signatures and electronic documents can be co-ordinated.

3.1.7 Special regulation

Certain problems could arise because the encryption algorithms used in producing digital signatures could be regarded as strategic products and thereby become subject to export bans. The rules which exist in this area are laid out in the report "E-money – issues concerning emittance"[15] The conclusions drawn in the report should, to some extent, be applicable in relation to digital signatures since, in both instances, it is authenticity rather than confidentiality which is the purpose of the technology. There may however be differences in relation to what the report had to take a position on.

[15] E-pengar – näringsrättsliga frågor, SOU 1994:14, section 4.10.1

3.2 The need for rules governing digital signatures and their legal effect

In order to allow regular use of the public telecommunication network for the transport of telecommunications messages in secure formats with the use of digital signatures, norms are required which ensure security. Such norms could be effected in several ways. One is through legislation with its consequent state regulation through secondary legislation or licensing requirements. Another is that market-led rules based on current legislation governing contracts, damages and other liability are created in the form of contracts between the affected parties. The former method would probably lay down rules more speedily, but could also hinder technological development and be perceived as more bureaucratic. The latter would probably be more flexible, but would mean that important questions of interpretation could remain unresolved over long periods. A suitable mixture of both methods could be preferable in order to provide legal stability without inhibiting development.

3.2.1 Paper documents – electronic documents

The Commission on Computer Related Crime described in detail the differences between the handling of traditional and electronic documents. Below is the Commission's account of the fundamental differences between the electronic and paper-based document.

Material thing – quasi-material object: Paper documents are material objects (things), whereas digitally represented information cannot be described in normal language usage as material objects.

Independent existence: Paper documents preserve text and details of their originator separately from other things, whereas the relationship between text, originator and bearer is not as fixed and unambiguous in the IT-environment.

Lasting existence: Paper documents fix their contents physically and enduringly in one way, whereas IT-procedures are structured so that stored information can be represented by data in processing and transfer phases of such temporary character that it cannot be regarded as an lasting object.

Unique existence: The paper document is produced in such a way that, in principle, only one unique physical original exists, while information technology is based on storing and transmission of original content.

Individual character: Paper documents have a greater or lesser degree of physical individuality, e.g. in the form of a signature, whereas in IT-storage there are no unique qualities other than those connected with patterns of ones and zeros e.g. in encryption.

Accessibility: Paper documents are directly legible whereas digital materialisation involves translation from machine language to legible form.

Representation form: Paper documents have writing as a uniform method of representation, whereas digital materialisations have several representation forms, both regarding technical solutions for representation in stored form (electronic, optical etc.) and readable forms (e.g. on-screen, print-out and voice simulation).

Susceptibility to internal manipulation, untraceable character, vulnerability: Manipulation of paper documents involves physical intervention which is traceable on a document, whereas changes in a digital materialisation involve an untraceable change in a bit-pattern on a data-bearer which it is possible to manipulate when transferring between different media.

Physical and logical context: Paper documents, when completed, contain a fixed constellation of a finite number of details which are put together for a defined informative purpose. In the IT environment, this fixed form is replaced by the possibility of combining and processing these details into an almost infinite number of variations.

Authenticity: Because of the physical link between the text and the bearer, a paper document can be examined forensically to establish whether it has been manipulated, whereas digital storage of information, without special precautionary measures, does not allow such an authenticity check.

Finality: When a document is produced, there is often a clear point of completion in the form of a signature or other statement of its origin directly linked to the text. Digitally stored information can be altered without trace, even if materialisation is controlled by a digital lock. There are no generally accepted procedures for verification.

Possession and tradition – symbolic functions: A paper document is owned (possessed) by someone who, in turn can pass (trade) it to someone else. The paper can thereby be the physical bearer of a right. This symbolic function is not normally re-created in the IT-environment where the transfer of data often involves a multiplication of the original material and not a physical trading of this IT-material. The corresponding legal effect is given by, for example, the rights to a certain item of property being registered as information in an IT-system.

Origin: The text in a paper document can be directly ascribed to human thought, whereas the information in a digital materialisation may be the result of automatic processes.

3.2.2 Written signature – digital signature

For the vast majority of people, the act of writing one's name on a piece of paper is seen as uncomplicated. The situations in which a signature is expected and what consequences this signature will have are often obvious, either through context or tradition. It is not unusual either for it to be expressly stated when a signature is required and what consequences this will have. In spite of this, it is not easy to describe and define the functions which the act of "signing" incorporates. There are descriptions of this in public reports and other literature. Below is a brief description of the more central functions and a short account of the extent to which the act of "digitally signing" can fulfil these functions.

Will: The act of "signing" can be regarded as the expression of a will to act in a certain way. The signatory gives his/her acceptance to the text placed before the signature. Closely linked to this function of will is the warning function connected with signing. The requirement of a signature often demonstrates clearly that a binding obligation is near at hand. In a similar way, a signature via the use of a secret key, e.g. a digital signature, is considered to be an expression of will. To what extent a warning function can be achieved in the use of a digital signature would depend on the general perception of whether a binding obligation will arise through this action.

Identification: A signature can be used to identify a person. This can take place, for example, through a signature written in the presence of a controller being compared with a signature which, with some degree of certainty, came from the person in question. Digital signatures too can be used to identify a person. This is achieved through the digital signature being verified with the open key. The connection between the key pair and a certain person must however be established – something which must be done by the CA.

Authentication: Through writing a signature on a document which contains a text, the text is connected in a certain way to the signature and thereby to the person indicated by the signature. The signature can thus be used to identify the person connected to the text. The fact that both the text and signature are fixed on the paper constitutes a certain protection against manipulation. The connection to a person results from the personal nature of the signature. The connection is not absolute however, in the senses that a signature is unique to an individual. A signature can be forged or two persons can have almost identical signatures. In order to establish a certain signature's connection with an individual, it is normally necessary to compare it with a signature which was definitely written by that individual. The possibility of detecting a forgery in this way varies. A similar phenomenon to the signature is the seal. It can be said to fulfil the same functions as a signature. From a control point of view however, there is a an essential difference between placing a seal or a signature on a paper. Whereas a signature can normally be checked after it has been

written, it is not possible to determine whether or not a seal was used by an authorised person. Like the impression of a seal, a digital signature can be used by anyone who has access to the private key. If several persons have knowledge of a private key, it will not be possible to determine which person signed. The signature is therefore not personal, but rather based on the person in question receiving a unique signature which he/she must keep secret. Under these circumstances, the digital signature can be used to identify the person who used the secret key. It also allows manipulation of the message to be uncovered, because the digital signature is connected to the signed message in such a way that possible changes in the message after signature can be detected.

Evidence: The identification function and the evidence function can be used in situations where the need for evidence arises, e.g. to verify the authenticity of legal documents. The placing of a signature on a document could be considered a way of securing any future proof of either the identity or the intention of the signatory. Digital signatures too can fulfil the identification and authentication functions and – in the same way as signatures – can be used in situations where the need to secure future evidence arises.

3.3 Regulation of CA-activities

In the case of CA-activities, required norms can also be established in different ways. The same views can be presented here as were applied to the question of the legal effects of digital signatures.

3.3.1 The key certificate's content and effect

Most of the suggestions which aim at the extended use of asymmetrical encryption for signing functions, i.e. over the public telecommunications network, are based on a trusted third party guaranteeing the link between the key and a certain person, i.e. a certification authority. This is done through the certification authority issuing a so-called key-certificate.

What is certified by the certificate depends above all on the form and content of it. The key certificate contains a number of items of information, including certain references to other sources. The character and scope of this information is presently not limited by anything other than the Data Act (1973:289) on the protection of information about the individual. In order for the certificate to fulfil its basic function however, it must contain a certain minimum of information signed by the certification authority. This information would, for example include

- the identity of the holder,
- the public key to be connected with this identity,
- the certificate's period of validity,
- information on the CA,

- how the certificate can be checked, i.e. information on the CA's public key and other checking mechanisms,
- a serial number and other information through which the certificate can be identified and checked,
- the conditions under which the CA issues the certificate, and
- policy (rules) for the issuing of certificates.

In order to eliminate any uncertainty in discussions concerning responsibility for the content in key-certificates, it is important that it is made clear *who* is considered the issuer of *what*. Any possible transfers of responsibility must also be clarified.

Particular problems could arise in cases where a certificate contains information about power of attorney. Two types of case can be discerned.

In the first case, the CA and the giver of the power of attorney are *not* identical. The information supplied is *about* the power of attorney and does in itself not constitute the granting of power of attorney. It would therefore still be the legal relationships behind this which would decide whether power of attorney existed or not. If the information contained in the certificate were incorrect, the question of liability would then arise in relation to anyone who had relied on this information.

In the second case the giver of the power of attorney and the CA are identical. This could be the case, for example, where a legal party who carries out the CA-function in his own business, certifies his own personnel. If the company issues a certificate to an employee, in which it states that the employee is authorised to carry out legal transactions on behalf of the company by using its digital signature, it could be argued that the certificate should be regarded as power of attorney. This is likely to depend on the form of the certificate if such is the case, or if it is only a matter of information about power of attorney as in the first case. In order for it to constitute the giving of power of attorney, it should however be a condition that the signatory of the certificate is authorised to represent the legal party (CA). The same reasoning could be applied to other actions by proxy.

For anyone considering introducing authorisation details to a certificate there are – irrespective of the above cases – reasons to carefully study some general problems which arise in relation to power of attorney. One example is how power of attorney can be revoked with binding effect in relation to a third party.

It might be of interest to consider whether it would be effective to introduce a public register of certificates with details of authorisation. One effect of this could be that registration could achieve certain legal force.

It is not completely clear who can be linked to a key. Should receipt of a digital signature be restricted to physical persons, or should legal parties be given the same right? If legal parties are also given this right, the question arises as to how it can be reliably demonstrated that a person is authorised to represent a legal party though using that party's key. Questions also arise in relation to the form of identity information.

Another question arises in relation to the legal effect of the content of a certificate in relation to a person who accepts a digital signature without checking the certificate. An example is the question of the extent to which a certificate can give rise to bad faith in the person who relies on a digital signature if this person does not check the content of the certificate.

The legal significance of the certificate will mainly be concentrated on its function as evidence. It is therefore important that the certificate receives a high degree of trust. Important factors in relation to this are:

- criminal sanctions against the corruption of certificates
- the right to receive financial compensation from CA if information in the certificate is incorrect, and
- the possibility of creating a method for verifying the contents of a certificate in a trial.

3.3.2 Infrastructure

Need for rules and checks

The confidence enjoyed by an identification document, such as a driving licence, may be said to depend on two factors. The document must be sufficiently reliable technically, i.e. difficult to forge, and the organization issuing it must enjoy public confidence. Rules to ensure this govern the issue of driving licences, which is the responsibility of the National Roads Administration. A driving licence must, for example, be plasticized and bear a photograph, which, together with other technical requirements, makes it difficult to forge. This creates a reliance on the driving licence which makes it possible to use it in a variety of contexts, despite the fact that the trusting party – e.g. a bank – does not itself have any involvement in the production of the identity document.

As with traditional ID documents, there have to be rules for the issue of electronic identity documents. An electronic identity document must be issued in accordance with a certain defined and generally known policy in order to be acceptable also to persons other than the organization which has issued it.

For a digital signature to have any legal value the first requirement is that reliable identification of the person who has created the signature must be possible, the second is that the key certificate must be correctly created, and the third is that the tools and the technique used in order to create the

signature are sufficiently safe. This means both that the function (CA) which identifies users and attaches a real identity to an electronic identity must be reliable and also that the programs/equipment which are used in the creation and verification of signatures must be reliable, if the signature is to have any legal value.

In future it is probable that more companies and organizations will wish to exercise the CA function. The question of what must generally be demanded in order to make digital signatures widely acceptable must therefore be answered – independent of which CA is responsible for certification.

Need for rules for the technology

To enable digital signatures to function in reality, technical standards and, possibly, rules of other kinds are needed for a number of different functions. It may not be necessary for all the undermentioned functions to be regulated by standards or statutes. In some cases it may be sufficient if the communicating parties are agreed on what should apply. This will however lead to greater uncertainty concerning the judicial assessment of a dispute concerning the validity of a digital signature.

Algorithms: To use a digital signature both a hash algorithm (or other unique "fingerprint") and a cryptographic algorithm have to be defined. As in the systems of many other countries, RSA is usually used in Sweden. In addition to the actual algorithm, certain parameters have to be specified. The length of the private key is particularly important, and so also is the public key. To some extent systems which verify digital signatures may contain different parameters, but the choice has implications for the confidence which may be placed in a digital signature.

Protection of signing keys: Strong protection may be provided by the use of smart cards, which are generally held to satisfy demanding standards of security for the recipient of the digital signature as well. In Sweden many have recommended the use smart cards for the protection of signing keys. In the USA however, there are also tried-and-tested systems with purely software-based handling of keys and signing function. The main reason for a standardization of electronic ID cards is probably the possibility of being able to ensure by this means that the holder of an electronic ID card can use it any system with no loss of security. Standardization permits cheaper products.

Personal code: Another example of areas which should be standardized is the processing of the personal code for the card's signature function. It is possible, as SEIS has recommended (see section 2), to have separate codes for the signing and the identification function in order to make sure that the user is aware when he is only identifying himself and when he is

signing a document. However it has been questioned whether it is feasible to require users to distinguish between two codes. If one is to allow the same code to be used for both functions, the structure of the personal code must be specified. It may consist of 4-5 digits or a longer string of alphanumeric characters. The latter alternative improves security somewhat, but eliminates the possibility of using the code in certain types of terminal which only have numeric keys. Some form of standardization is in any case required in both the cases described.

Key certificate format: The format of the certificate is often based on one international standard (e.g. ITU/X.509). As several variations of the standard exist, a choice has to be made. The choice depends on security considerations but also on practical matters such as the identity concept to which the digital signature is primarily linked. It is possible for instance to allow a certificate to be linked to an identity (e.g. a number), which is in turn linked to a natural person or legal entity.

Methods of revoking certificates and checking revoked certificates: To check whether a certificate has been revoked, public directory services are usually employed. However these may have different interfaces and different rules regarding access, which means that there is a need for review and harmonization in order to facilitate their use. In addition methods of revoking a certificate must be defined.

Formats for linking signature and any certificate to the signed information in order to create a digital document: The area contains a number of international standards which are not particularly well developed. Nor is this important from the security point of view. A number of different formats are possible. However it is important in practice for the recipient of a signed document to have a technology which makes it possible to read text and verify signatures in a correct manner.

Methods of checking security in the system which is used when signing: There are a number of threats which make it impossible to be entirely sure that the signing system used really guarantees that the contents which the signing person intended to sign agree with the content of what has been signed. A comprehensive control of this problem is very difficult and requires far-reaching standardization of application programs and hardware and, probably, an independent control of the technical realization of the system.

Rules for the administrative infrastructure

To enable the parties to have confidence in the digital signature it is important to have rules for how certificates and electronic ID cards are to be issued. Efforts are being made in ETSI[16] and IETF[17] to create technical

[16] European Telecommunications Standads Institute

standards in this area. The work on standardization is concerned more with creating a concept model for trusted third-party services than with defining the contents of a system of rules. This is being left to the parties themselves. The international efforts which are being made to create standards in the area describe in general terms the certification process and the need to protect private keys.

Possibly one should look for other ways of deciding on a system of rules, rather than the formal standardization process. However there is nothing to prevent other procedures being made the subject of standardization. Examples of this are to be found in standards of quality assurance in administrative processing which have been set up in the ISO 9000 series.

A system of rules for administrative processing needs to be able to answer a number of questions. For example:

- On what basis should certificates/ID cards be issued?

- How should it be possible to check the identity concept which is being used?

- How is the identity of the applicant checked?

- How is the CA to arrange protection and inspection of the system and the keys which are used when issuing key certificates?

- How are signing keys of sufficiently good cryptographic quality and with satisfactory protection against abuse to be generated? Should these only be registered on ID cards and then be locked against all external access?

- How can hackers or others with specialized knowledge on the manufacturing side be prevented from misusing the physical card product?

- How does one protect ID cards being transported from central personalization to the place of delivery.

- What possibility should exist of changing PIN code?

- How is it to be ensured that information on revoked certificates is available to those wishing to carry out a check?

These are examples of questions which may be specifically dealt with in a security policy for a trusted third-party service. Such a policy might exist in the form of a standard.

[17] Internet Engineering Task Force

CAs and archives

If we assume that the problems of long-term preservation – which have been mentioned in section 3.1.5.2 with particular reference to the difficulty of preserving the legibility and authenticity of digital messages/documents – can be solved, there remains the question of how the information on keys etc which CAs handle is to be dealt with in the long term. To what extent should this information be transferred to state or municipal records office departments when there are no longer commercial reasons for preserving outdated information? In order to retain confidence in digital documents even in the long term, the measures employed for creating this confidence must also be capable of being documented and preserved. This applies even after a CA activity has been wound up.

The signature is crucial to the authenticity of a digital document. The security with regard to the origin and content of the document which the signature is intended to create may be inadequate, however. Additional confidence-creating functions need therefore to be preserved. In addition to documentation of keys, documentation showing who has actually been certified needs to be preserved. Otherwise there is a risk, not only that messages from individuals who have had certificates may be subject to forgery or distortion but also that entirely new messages may be created where the supposed issuer has had neither key nor certificate.

In these circumstances it appears necessary, as far as archive storage is concerned, to consider carefully what measures are required in connection with the winding-up of a CA. To some extent it ought to be possible to compare the questions arising here with those concerning the end of the millennium. What may at present appear unrealistic and exaggerated may in the rather longer term prove to be considerably more serious and urgent problems.

3.3.3 Certification and inspection of CAs

This section will deal briefly with the manner in which inspection (supervision) of CA activities may take place. "Inspection" also raises the matter of certification or licensing of CA activities.

Inspection may be carried out by the body which certifies a CA. In a hierarchical system, for example, a superior CA lays down conditions for the certification of a subordinate CA. However cross-certification would seem to present a somewhat different situation. Considerations of competition make it appear unlikely that participating CAs could supervise each other.

Alternatively inspection may be carried out by an autonomous body. The supervisory function may be governed by contractual or public law.

Licence for CA activity

Operators may be licensed either following an application or by self-licensing. Licensing may be compulsory, i.e. a precondition for carrying on CA business. The activity must then be defined in some manner. Rules concerning licences may also be facultative (voluntary). Only licensed CAs are then affected by certain statutory requirements. Under a facultative licensing regime it is probable that digital signatures emanating from a licensed CA will enjoy a higher degree of trust than those from non-licensed activities.

A licensed CA business concept raises a number of fundamental questions. Some of the more important ones are the following:

- Who is to be authorized to apply for a licence? Should it be a state, an inter-governmental organization, e.g. the EU, an international organization or a private individual?

- Should all CA business be subject to obligatory licensing? International agreements – e.g. Article 59 of the Treaty of Rome and the WTO Treaty – on free mobility of services may affect rules prohibiting unlicensed CA business, as may rules on fair competition and rules against the formation of cartels.

- To what extent should the licensing body be liable to third parties for the content of a certificate? By attaching conditions to the licence – a licensing schedule – the licensing body may be obliged to undertake necessary examinations of CAs. This may in turn give rise to the question of the liability of the licensing body to the person relying on a certificate. On the other hand confidence in a certificate may be increased by the fact that the licensing body is responsible for it.

- Should only certain specially trusted agencies or professions be allowed to engage in CA business? Trust in a certificate might be increased if CA business could only be carried on by already trusted categories who are subject to some form of supervision. For example Public Notaries, lawyers or banks. Such rules may affect questions of liability.

- To what extent should CAs be empowered to regulate their own business? For a CA to function effectively it must be provided with the power to draw up rules binding those whose certificates it certifies. This can be achieved by contracts. However the effectiveness of this and the possibility of enforcing contractual obligations may conceivably be questioned.

– Does CA business need to be regulated? One possibility is that of relying on the self-regulating ability of market forces. A party which abuses its trust will not in the long term be able to continue in business. Another possibility is to leave it to the market – for example by means of branch organizations – to regulate activities itself. If instead a national legal regulation is chosen, this is likely, in view of the international character of the CAs, to require a harmonization with other countries to prevent rule conflicts.

Requirements for obtaining a licence

To satisfy users' interests and the ensure the security of the system etc., requirements may be imposed on those wishing to obtain a licence. The requirements should be so formulated that the certificates issued can also be accepted in other countries. In Sweden's case it may be valuable if common criteria for CA business can be laid down at Community level. This would mean that certificates issued in one member state would be recognized in all member states (reciprocal recognition). In the communication "Ensuring Security and Trust in Electronic Communication – Towards a European Framework for Digital Signatures and Encryption"[18] the Commission has given the following examples of such common requirements:

– security in the CA and compliance with data security legislation,

– reliable identification of individuals (to ensure that a particular key holder can be identified),

– lowest level of insurance cover (the CA must be able to pay a possible indemnity),

– technical components,

– training and security control of staff, and

– prohibition of "self-certification" of CAs.

The Commission found in the same communication that it might be appropriate – in order to achieve maximum security – to make a clear distinction between different tasks, e.g. certification and key depositing, and between different types of certificate. The schedule of requirements ought therefore to vary according to the services which are offered by the CA.

[18] COM (97) 503 final

In addition to the requirements pointed out by the Commission in its communication, some form of regulation of the following areas is also likely to be needed.

Documentation: Necessary documentation concerning identification, date of issue of certificates, date when certificates cease to be valid, cancellation or revocation of certificates, technical procedure for producing certificates, date stamps etc., as these may need to be proved at legal proceedings where representatives of CAs may be called on to give evidence. Regulation may need to state the time during which the documentation has to be preserved. Account must be taken of rules regarding statutory limitation. Rules concerning the preservation of documentation, together with back-up routines and similar security measures, may be needed.

Audit: The CA's business should be audited regularly. The question arises of whether existing legislation on obligation to keep accounting records etc. – with the possibility of auditing – is adequate or whether special auditing rules are required. If special rules are introduced the question of whether auditing should be carried out by private auditors or by the licensing body arises.

Supervision and enforcement: Whether regulation is arranged in the form of self-regulation or through licensing, the right of an organization or authority to exercise supervision and take enforcing action must still be properly based in law.

Appeal: Every form of rules system would seem to need to contain the possibility of appealing against decisions. Rules of procedure need to be introduced.

Charges: CAs appear likely to charge for issuing certificates. Questions of price regulation may arise. Charges by the state may in certain cases constitute disguised barriers to trade in services.

Termination of CA business: In the event of a CA discontinuing its business, rules may be needed concerning obligation to surrender documentation and certificates to another CA or obligation to retain documentation and retain evidence of certification for a certain time.

Inspection of technical products

Technical products intended for use in producing digital signatures must as stated in a previous section satisfy certain requirements. To ensure that the requirements are satisfied an inspection function is required.

The German law on digital signatures (§ 14) reveals in broad outline what needs to be inspected. Insistence on such inspection is likely to arise

irrespective of whether the business is operated with or without a licence. If the business is licensed the technical control required may need to be more closely defined. The German rules stipulate that certain technical components must be checked against certain demand levels. The algorithms and accompanying parameters which may be used must be made public. The inspections must be carried out by special approved testing agencies.

Sweden has a law (1992:1119) on technical inspection. Assessment of compliance and other technical inspection is carried out under the law by, or with the assistance of, a body as referred to in section 1, paragraph 1 of the law, or by an accredited body. This applies provided that inspection is prescribed by law or other statute, has been imposed on a party by a decision of a public authority, or otherwise has special legal effect under the provisions of law or statute (section 2). There then follow rules concerning which bodies should be notified to the EU. Such bodies must test compliance with regulations which apply within the EEA. The law is accompanied by an ordinance, in which it is stated that authorities which may prescribe that products, systems etc. must have or must not have certain characteristics (prescriptive authorities) shall consult the Board of Accreditation and Technical Inspection (SWEDAC) before issuing directives on assessment of compliance which are covered by the law on technical inspection.

SWEDAC is the national body for accreditation under the law on technical inspection. There is an instruction relating to SWEDAC. In addition there is an ordinance (1989:527) on national testing agencies and national measuring agencies, which now applies only to national measuring agencies.

The law on technical inspection could be applied to technical components for the production of digital signatures.

Inspection of CA business

CA business embraces both administrative procedures and the use of technical components. However, inspection of CA activity can include checking whether the technical components utilized fulfil certain requirements.

A market-regulated inspection of CA business might conceivably take one of two forms. In the one case the CAs agree on a joint inspection body. In the other, inspection is in the hands of the CAs, which cross-certify each other. A CA which shows inadequacies may thus be excluded from the

joint scheme. In view of the competitive situation, it would appear difficult to institute a real supervisory function of the latter sort.

If the CA business is regulated by law, a supervisory function can be instituted. Such a function would likely include inspection of compliance with requirements laid down for the business. Inspection may take place when business starts, in conjunction with allocation of licences and by means of regular or random ongoing inspections of the business.

3.3.4 Recognition of foreign CAs

For electronic commerce to be able to function internationally, certificates issued by foreign CAs must be recognized in other countries. For the EU this means that national structures can be supplemented by coordination in this respect at Community level. For the member states, agreements with third countries are also necessary.

Mutual recognition of foreign CAs

One difficulty in connection with recognition of foreign CAs is that it may be difficult to detect inadequacies in the foreign supervisory apparatus. A failure in the foreign inspection function may undermine confidence in the whole system.

Questions which may arise in connection with the recognition of foreign CAs include:

- How will cultural differences affect recognition?
- What requirements must be laid down in order for foreign certificates or CAs to be recognized?
- How should one proceed when one judicial system contains an obligatory requirement for licensing while another does not?

Mutual recognition of licensing procedure

One possible route to regulation might be to introduce a standard for CA activity. This will make it possible for CAs from different jurisdictions to rely on certificates which have been issued in accordance with the same standard. It should however be borne in mind that the certification process involves human action in various respects, which may lead to significant variations in the manner in which such standards are *de facto* applied. Will it therefore be possible to accept a foreign certificate, which in itself satisfies the same standard as the domestic one but which originates in a country which lacks a reliable organization for personal identification?

Recognition through standards does not mean that all CAs must have a licence. In certain legal systems licensing of CAs may be obligatory, in others voluntary or entirely lacking. What determines whether a foreign CA should be recognized is the reliability of the licensing scheme. In order to assess whether all, some or no CAs in a particular country should be recognized, the legal system of that country must be studied.

Recognition of foreign digital signatures in practice

The courts will in all probability be faced with the question of the reliability of a digital signature. Especially when the signature comes from a country which lacks rules on recognition will the demonstrating of the reliability of the digital signature be a costly process.

A European framework

In the EU the Commission has proposed a European framework for digital signatures and encryption in the abovementioned communication "Ensuring Security and Trust in Electronic Communication – Towards a European Framework for Digital Signatures and Encryption".

Within the EU there are two possible ways of promoting international electronic commerce by judicial means. The member states may in their national legislation themselves introduce rules on mutual recognition of foreign certificates. An application of articles 30, 52 and 59 in the Treaty of Rome will to some extent prevent the introduction of special rules in individual member countries if they restrict competition. Another possibility is that of taking action at Community level to harmonize a European CA activity, and also introducing common criteria and procedures for evaluating such activity. Such harmonization may take place with the support of directives. A directive is binding on the member states.

Using national legislation may however give rise to problems. A not altogether impossible example might be that a member state introduces a legally regulated licensing system for CAs which does not leave room for a recognition of certificates from other member states. To facilitate mutual recognition a solution at Community level may be of value.

3.3.5 Powers of supervisory bodies

If CA activity is regulated by law, with requirements being imposed regarding how business is to be operated etc., a supervisory function probably needs to be introduced. For this to be effective the supervisory body must be equipped with powers which make it possible to carry out the supervisory function and take action against a CA which does not observe the rules which apply to the business.

Examples of such powers might be the right to

- demand documents and carry out inspections,
- issue directives concerning the activity and technical products,
- issue injunctions, possibly accompanied by sanctions,
- prohibit certain activities,
- revoke licences,
- block certificates, and
- report for prosecution.

In addition it should be considered whether there needs to be a possibility of compulsory administration of a CA business for a transitional period, possibly combined with a power to transfer the business or wind it up.

Rules for supervision of the finance sector may be of guidance in designing rules for the supervisory operation here.

3.3.6 Liability issues in different party relations

Problem description

The use of digital signatures brings to the fore a number of different party constellations, where current law concerning liability issues is uncertain.

The relationship between *trusting party and keyholder* is unclear in the case where an unauthorized person misuses the private key component. The misuse may for instance have been made possible due to the underlying technology being easy to manipulate or due to the keyholder having been careless with his or her PIN code or smart card. According to Swedish law, the starting point should be that the keyholder is not bound by legal acts not undertaken by him.

The relation between *CA and trusting party* may be of different kinds. It may be contractual, non-contractual, quasi-contractual, indirectly contractual or subject to the provisions of the Administrative Procedure Act – depending on the situation. If the relation between the CA and the trusting party is contractual freedom of agreement prevails. A description of the relevant rules is provided for in section 3.3.7. In most cases, however, a relation based on contract law is probably not at hand. In non-contractual relations the point of departure is that liability for pure capital damages exists only in cases when the damage is caused through crime. A 1987 court case[19] shows, however, that there are cases when protection is called for persons who, without being contracting partners, have a closely connected and protection-worthy interest in having the contract fulfilled.

[19] *Nytt Juridiskt Arkiv* p. 692

Whichever way the relationship is categorised, the apportionment of liability is uncertain. The question is, for instance, what type of responsibility does CA have for the keyholder's identity and for the messages being unchanged. Is it a matter of strict liability, culpa liability, exculpation liability, or liability only if CA has acted in a criminal way? In addition, there are problems and uncertainties relating to the extent to which, and if so how, CA can limit his liability. In this connection, there may be a difference depending on whether the trusting party is a consumer or a business.

The relation between *keyholder and CA* is the least problematic. It is contractual and both party's obligations can be settled in the agreement. If the CA does not meet its requirements according to the right of contract, a breach of contract has occurred. The consequences of this is settled in the agreement, possbily supplemented by e.g. general principles of contractrual law. In the commercial sector, contractual freedom is restricted ultimately by the so-called general clause in section 36 of the Contracts Act. If the keyholder is a consumer, it is conceivable that there are further restrictions to contractual freedom (cf the Consumer Sales Act or Consumer Services Act).

Another issue is the extent to which it shall be possible for CA to revoke or temporarily block a certificate without the keyholder's explicit request.

A situation may arise in which an unauthorised person assumes the identity of a certain person who has never been in contact with CA. The question then arises of *CA's liability in relation to the person whose identity has been misused*. While it is the case that the person who suffers such misuse is not bound or responsible to the trusting party, he may none the less suffer considerable damage, for instance due to his creditworthiness being called into question. The contours of CA's liability are uncertain, if the CA, for instance, has acted without due care when checking identity.

Description of needs

As has been made clear, the legal situation is to some extent uncertain with respect to the liability in the relations arising due to a digital signature. A more detailed analysis of the legal situation is required and whether legislation is necessary or whether it can be left to court practice. In this context it should be observed that the need for civil law legislation is affected by how CA activity is regulated. This need is particularly accentuated when the keyholder is a consumer. A starting point for further analysis should be the maintenance of a strong consumer law protection.

In this context, it should be pointed out that the German legislation on digital signatures does not deal with liability issues and that this was an active taking-of-position on the part of the German legislator.

The American Bar Association

The American Bar Association has in a document entitled ”Guidelines”[20] proposed a regulatory framework for CA activity. Guidelines contains the basic rules for CA. One of the rules contains a limitation of liability for CA.

According to the Bar Association, a dividing line can be drawn between the damage cases which are a consequence of CA being in breach of the rules laid down for the activity and such damage which has occurred despite CA abiding by the rules.

According to the Bar Association, a CA, who complies with applicable legislation and, where relevant, contractual conditions and the regulatory framework contained in the Guidelines, shall not be able to be held responsibility for damage, which

1 the holder of a certificate or another person has incurred, or

2 is caused by someone relying on

– a certificate issued by CA,

– a digital signature which is verified with the aid of a public key which is specified in a certificate, or

– information provided in such a certificate or at a repository.

The possibility of limiting CA’s liability in this way is essential according to the Bar Association to stimulate the establishment of CA activity. According to the Bar Association, few would dare risk investing in an establishment without sufficient clarity on the basic rules and the ability to estimate the legal risks.

3.3.7 The liability borne by the state

A question that may arise within the framework of a system of digital signatures is what liability the state bears in the event of major damages. The answer to the question is to a great extent due to the role of the state and how this system is legally structured. Another issue of interest is what applies with respect to the state’s liability in the event of CA’s bankruptcy.

[20] Digital Signature Guidelines – Legal Infrastructure for Certification Authorities and Secure Commerce, 1996, American Bar Association, Chicago, USA

There follows below a brief description of the current legal position in the stated areas.

Major damages – the state acts as CA

If the state (or a government agency) assumes the role of CA, the state may – like any CA – be liable to damages. The nature of this liability may assume different forms depending on the legal aspects of the system, etc. As has been shown above (see section 3.3.6), such liability *in relation to the signing party* may be based on purely contractual considerations. Liability is in this case regulated in the agreement between the parties, possibly supplemented by general contractual considerations. In this case, there is freedom of contract, which entails that the parties can settle all relevant issues such as grounds for liability, the scope of liability, limitations to liability, etc. at their own discretion. If the parties have not regulated these issues – which seems per se less realistic – a discussion can take place on the liability borne by the CA. The answer is not obvious. It depends *inter alia* on how the contract is otherwise drafted. As a ”minimum level”, it can be said, however, that CA is at least liable for damages in significant breaches of contract.

In the commercial area, freedom of contract is ultimately restricted by the general clause in section 36 of the Contract Act, which makes possible modification of unreasonable terms of contract. In those cases where the signing party is a consumer, it is conceivable that there are further limitations on freedom of contract (cf the Consumer Services Act). What has now been said applies regardless of whether the state assumes the role of CA or not.

Another question is whether the state has any further responsibility beyond what applies in general or if the state’s liability is limited in some special way.

As long as the relationship between the state (in its capacity of CA) and the signing party is to be regarded as falling under the right of contract, the responsibility of the state does not extend further than what follows from general principles relating to the law of damages. The Tort Liability Act, which *inter alia* regulates the liability of the public authorities, does not in principle apply to internal mandatory (contract law) situations (Chapter 1, section 1).

Furthermore, the question arises of the state’s liability in relation to the *trusting party*. The relation between the trusting party and CA can per se be based on the right of contract. In this case, the principle applies as explained above. However, there is not usually any contractual relationship between CA and the trusting party. In such cases, the general provision on the state’s (public body’s) liability for damages in Chapter 3, section 2, of the Tort Liability Act is relevant. This section makes

provision for central or local government, to compensate personal injury, property damage, or damage solely to wealth (non-related to personal injury or damage to a material object), which has arisen by error or neglect in the exercise of public authority for whose fulfilment, the state or a municipality is responsible. This means that there is difference compared with if CA is a private subject. A criminal offence is not a prerequisite for central government's liability for damage solely to wealth, which is the case if the CA is a private subject (cf Chapter 2, section 4, of the Tort Liability Act). The state's liability accordingly goes further to that extent. It is, however, a requirement for liability that the damage has arisen in the course of exercise of public authority. This requirement may act as a restriction in some cases.

Otherwise, it may be mentioned that special provisions exist (or can be expected) for areas that are very similar. In the proposed legislation on personal information (Government Bill 1997/98:44), a provision is proposed (section 48) that a person responsible for personal information shall compensate a registered person for harm to and encroachment of personal integrity which processing of personal particulars in breach of the law have caused. This liability to compensate can be moderated if the person responsible for personal information can show that the fault was not due to him. The Personal Information Act will probably not be applicable to digital signatures since these are not regarded as personal information (cf section 3). However, it is expected that the damages construction will be copied in more systems of records.

A 1993 Government report (SOU 1993:55) contains a proposal that central or local government shall compensate damage solely to wealth which has been caused by error or neglect when an agency has provided information. This proposal is at present being prepared by the Ministry of Justice.

Major damages – the state's liability in other cases

If the state does not have the role of CA, the situation is different. The state has no special liability for damages in the event of, for instance, major damage. Special legislation will be required if it is wished to create such liability. Various "guarantee constructions" can be mentioned from other areas, for example, the deposit guarantee an account-holder at a bank has.

Finally, it may be mentioned that the situation can be different if the state – without being a CA – forms part of the system in any way. If, for instance, the state exercises supervision or the like, the state can be held liable for damages in the event of deficiencies in carrying-out of its supervisory function. This depends on how the supervisory function is organized and regulated.

The state's liability in the event of a CA's bankruptcy

If a CA is declared bankrupt, possible claims for compensation is entered as a proof of debt in the bankruptcy. The bankruptcy estate is not liable for such. The state has – apart from the employee's right to a wage guarantee – no special liability in such cases.

4 Alternatives for action

After this review of technical and organizational prerequisites, and the legal and other societal aspects with respect to digital signatures, some main features of the various alternatives for action can be distinguished.

The demands that can be made on the use of digital signatures depend on the context in which they are to be applied. Is it to take place in open networks or in closed circuits of users? What type of transactions are the digital signatures to be used for and are there any limits as to the extent or importance of such transactions may be.

4.1 Allowing the market be responsible for developments

The difference between alternative systems and actors means that there is not necessarily any uniform answer as to whether the market or the legislator should design the regulatory framework for digital signatures. Systems such as PGP which largely lack a CA function in the meaning of the concept applied here, should have a clear function to fill and there may be no reason to introduce regulations for such activity. An aspect which should be taken into account, however, is the systems' development potential.

In certain contexts however, it is probably a prerequisite for all systems with digital signatures to be able to function that the general public feel confidence in them. In order to establish confidence in digital signatures, a number of factors must be complied with. First and foremost, reliable technology is needed, and a reliable organization for identification of certificate holders, and for handling key certificates and catalogues, etc. There is reason to believe that the market can manage to establish qualified organizations with access to the requisite technology to be able to produce safe digital signatures. It can also be expected that the market will solve questions concerning the division of liability in contractual relations between CA, the keyholder and the trusting third party. One question is, however, whether everyone's interests will be catered for in a satisfactory way through such solutions. Balances will be struck between interests by writing contracts, and through court practice, in which context it can be expected that a balance will be struck as to what is equitable. If such a market-controlled development leads to inequitable results, civil law legislation can be used to protect users, especially consumers but also business users to a certain extent. The market can in part solve the problem with major damages by insurance, and by only allowing very large businesses and organizations of good standing to be entrusted to act as CA.

It may be assumed that it will be more difficult for the market to solve such issues as liability in non-contractual relations between CA and a trusting third party. Moreover, it may be uncertain to what extent a CA can be released from liability without the backing of the law. An even more important question which the market cannot solve on its own at all is to increase confidence in the system of digital signatures by, among other prerequisites, increasing the level of sanctions compared with more general offences which such a way of action may form part of, for instance, fraud. Other issues which the market can find difficult to resolve on its own are integrity issues. What information about a user and his use of the system shall a CA be permitted to store and what protection applies against making such information available to outside parties?

Another matter which only a legislator can achieve is some kind of rule of presumption with respect to confidence to digital signatures under certain specified conditions. However, it may be called into question whether such an order is desirable taking into consideration that the rules of the Swedish legal system have functioned fairly well until now with respect to where the burden of proof shall be placed.

To change the principle of free examination of evidence is quite out of the question.

Large start-up costs for CA activities and the possibility of coping with major damage claims, can result in only a smaller number of companies being prepared to serve as CA in such systems where there is a high demand for reliability. This can provide security for users. At the same time, it can be an obstacle to competition. One aspect which may be worth mentioning in this context is that a state-owned company such as Sweden Post AB and Telia AB can obtain a competitive advantage precisely by being state-owned.

4.2 Legal regulation

When designing a possible legislation on digital signatures a problem-oriented perspective should be used. This means that legislatioin should only be made in cases where it is needed and, for each problem which can be identified within the area, it should be considered whether legislation is the most appropriate solution or not.

Legal regulation of digital signatures consists of separate parts.

- In the first place, regulation to carry out CA activity.

- In the second place, it concerns the effects of a digital signature; both the legal effects in the case where form requirements of a pen signature or on a written document can prevent the use of digital signatures, and the effects of evidence.

– In addition, there may be some other regulation linked to law enforcement activities and export controls on stategic products.

4.2.1 Regulation of CA activity

No proposals have been made at present relating to regulation of CA activity in Sweden. However, there are a number of foreign laws in this area. A proposal from the European Commission for an EC directive on digital signatures which will probably include a licensing procedure is expected in the near future. According to the regulatory framework which has been worked out concerning digital signatures and encrypting, this directive may either be focused on what in this context mostly closely resembles a regulation of CA activities but it may also entail that member states are to harmonise their legislation so that digital signatures are to be put on the same basis as traditional signatures. The latter alternative is much more far-reaching and can require a longer period to implement. On the other hand, it is evident from what has been said on international private and procedural law that a uniform legislation in the member states would simplify matters for users of a system for digital signatures.

The legislation introduced in Germany is an example of regulation of CA activity with general application. The German model can be applied to Swedish conditions. It may have certain disadvantages due to its wealth of detail making it technology-dependant. Much of the detailed regulation has also been included in the ordinance, which is easier to amend. An example of legislation where there has been an endeavour to make it independent of technology is the Californian. It should be endeavoured in any case to make legal provisions as independent of technology as possible. Inter alia the demand for use of smart cards should not be regulated by law.

Limitations to the area of applicability for digital signatures, whenever requirements on form exist, can however be made, such as is intended in part I of the report Electronic Document Processing[21] – restricting its introduction to the case-handling by government agencies. This is also approximately what has taken place in, for instance, California's legislation.

Some guidelines for regulation of CA activities have been given in section 3.3.

The investigation into electronic money has in its interim report E-money – legal issues concerning emittance[22] provided general proposals for a regulation in law of (systems for) issuing electronic money. Annex 3 of the interim report contains a sketch of how such regulation could be

[21] SOU 1996:40 Elektronisk dokumenthantering
[22] SOU 1998:14 E-pengar – näringsrättsliga frågor

organized. Much of what is proposed could also correspond to the legislation for CA activity in systems with digital signatures. Certain differences would exist, of course, since the proposal on electronic money concerns a part of the financial sector while CA activity can be a more comprehensive activity that extends over all sectors of society and may therefore have consequences that are more difficult to overview. At the same time as issue of electronic money may seem an activity of such high importance for society that a license is to be required to carry it out, it is not certain that this need be the case for CA activity, etc. Finally, a statement is made, in connection with the sketch in Annex 3 to the interim report on electronic money, that the issue of norm-giving competence needs to be clarified. The equivalent applies in a regulation of CA activity, since it should there be a matter of striking a balance between how much is to be regulated by statutory act or by ordinance or regulations.

A regulation of CA activity may also be linked with the legal (and evidential) effects of digital signatures in such a way that it is for instance only digital signatures produced with support of key certificates issued by a CA which has a licence according to legal regulation that benefit from a more severe penalization in the event of misuse, which may be used according to the Administrative Procedure Act, etc.

4.2.2 The effects of digital signatures

The legal effects of digital signatures

The first question that may be asked is whether a digital signature – if it complies with a certain level of security – shall generally enjoy the same legal effects as a pen signature. There is a benefit in a method of legislation, which has this effect. All the laws and regulations that contain a requirement for a signature may be included at once in the use of digital signatures by an amendment to the law that equates them to a pen signature. On the other hand, the introduction of such a legal provision where the technology has not been tested on a large scale in open networks in transactions of all possible kinds could have unexpected consequences.

In the light inter alia of the different reasons underlying the formal requirements in different legal provisions, a provision with a general application entailing that digital signatures are accepted instead of pen signatures is probably not feasible.

With respect to the legal effects of digital signatures, legislation has already been introduced in a number of areas where electronic documents are accepted instead of documents with pen signatures. What these administrative law provisions all have in common is that the law is to be applied by a government agency which also has an influence over the rules on computer-based document processing, and the agency can issue

more detailed instructions as to how this processing is to take place. Ultimately, the agency can require that written documents are submitted. Even if the regulations are similar there are discrepancies, which lead to what is applicable in one agency, not being automatically applicable to another agency, which is subject to other legislation.

Proposals for generally applicable regulations for digital signatures are contained in the Commission on Computer Related Crime's report regarding penal law. In the proposals for amendment of the Penal Code, definitions of documents are recommended that include, in addition to written original documents, a set quantity of data for computer-based information processing, if it is possible to establish from the content who is the issuer. According to the proposals, such a document can be created by the use of digital signatures. The recommendations do not include any rules on the more detailed requirements that a digital signature is to meet to comply with the document concept. The work of standardisation that is in process with regard to digital signature is mentioned. At the same time, it is made clear that even non-standardised digital signatures may entail the existence of a digital signature which can meet the requirement for a document in the proposal for a new Chapter 14, section 1, of the Penal Code, on document forgery or the requirement for a signature pursuant to the proposal for a new Chapter 14, section 9 of the Penal Code on falsification of signature.

The report Electronic Document Processing also contains a proposal for general legislation in administrative law. In this report, it is proposed that a number of definitions are included in section 1a of the Administrative Procedure Act, including on digital signatures – the result of a change of an electronic document making it possible to check whether the content originates from the physical person stated as the issuer. Neither are any more detailed rules proposed here as to the detailed requirements that must be met if a digital signature is to be considered to exist. The authorities should, according to the proposal, keep the right to require that a message which lacks the sender's signature in original form should be confirmed by a document being signed in original form. The proposal is limited to the processing of cases by government agencies. The judgmental activities of courts are excluded, for instance. According to the proposal the Government shall, regarding such procedural rules that exist in laws other than the Administrative Act and thus according to section 3 of the Administrative Act enjoy preference over the latter, have the right to authorise affected agencies to specify that requirements for traditional written procedures may be carried out electronically. To date developments in this area of the proposal, as mentioned above, have instead taken place by amendments being made to the special laws, that apply to each subject area.

Evidential effects of digital signatures

With respect to the evidential effects of digital signatures, it should only be a matter for the legislator to draw up rules on the burden of proof, for instance, in the event of a denial of a digital signature. It can hardly be anticipated that there are reasons, with respect to the area of use of digital signatures, for deviating from the rules of evidence that are otherwise applied. It would therefore seem not to serve its purpose to lay down special rules on the burden of evidence which deviate from those applicable today to falsification objections. No legal regulation should therefore be made regarding the burden of proof. The benefits from the point of view of evidence that can be obtained from structured procedures to achieve digital signatures with a given level of security can nevertheless be considerable. Of special importance in the area of evidence, is the extent to which the system can be audited for individual cases where the genuineness of the digital signature is called into question.

4.2.3 Other regulations

Digital signatures are intended to assure the issuer's identity and the authenticity of the message received – not to create confidentiality. However, it cannot be overlooked that the methods for securing identity and authenticity and confidentiality are also based on the same technical procedure. A possible regulation of digital signatures could therefore become dependent on how a policy on encryption for confidentiality is designed.

Encryption for confidentiality is a complicated issue and it will probably take time before Sweden and other countries have decided on national policies. In order not to delay developments in the use of digital signatures, the two functions should be separated for the time being. A separate treatment of signature and confidentiality functions is also the orientation which the international regulation has for the time being (cf Germany).

The requirements for integrity for the holder of signature keys can probably be met by key deposit not being required for the digital signature system at the same time as the need of the police and other investigating authorities to be able to tap telecommunications is not counteracted by the use of keys for digital signatures being limited by technical procedures. The use of keys for digitial signatures can be restricted through technical procedures whereby signature keys cannot be used for confidentiality encryption of messages.

Probably it is not possible to achieve a 100 per cent protection against misuse of keys. It may therefore be necessary to complement the technical procedures with particular rules on the use of keys, e.g. an explicit prohibition against using signature keys for confidentiality encryption, and clear requirements on CAs to provide separate certificates and key pairs

for the two uses. A possible measure is to link the use of keys to liability rules.

When condisering how extensive the requirements on technology and use should be in order to fight against crime, a balance must be struck between the value of an efficient law enforcement and the costs incurred by more expensive technology and restricted flexibility for the users.

The rules for export of goods with dual areas of use, for example strategic products, and their importance for use of digital signatures must be studied. The same considerations as above regarding technical possibilities to prevent misuse of signature keys also need to be made in this respect.